REMARKS

Reconsideration and allowance of this application are respectfully requested in light of the above amendments and the following remarks.

Claims 1, 20, and 29 have been amended. The amendment of claim 1 has been drafted to overcome the objection applied thereto. Support for the amendments is provided for example in paragraph [0002] of the published specification. (References herein to the specification and drawings are for illustrative purposes only and are not intended to limit the scope of the invention to the referenced embodiments.)

A Terminal Disclaimer is enclosed herewith to overcome the obviousness-type double patenting rejections applied to claims 1-7, 9, 10, and 15-42.

Claims 1-7, 9, 10, 15-17, 19-39, 41, and 42 stand rejected, under 35 USC §103(a), as being unpatentable over DiGiorgio et al. (US 6,385,729) in view of Graham, Jr. et al. (US 6,402,028) and Elgamal et al. (US 5,657,390). Claims 18 and 40 stand rejected, under 35 USC §103(a), as being unpatentable over DiGiorgio in view of Graham, Elgamal, and Brown et al. (US 5,455,863). The Applicants respectfully traverse these rejections based on the points set forth below.

Claim 1 defines a system for establishing a communication pipe between a personal security device (PSD) and a remote computer system over a network having a local client serving as a host for the PSD. The local client connects the PSD to the network and: (1) separates encapsulated APDUs from message packets that are received from the remote computer system and communicates the separated APDUs to the PSD, and (2) encapsulates APDUs received from the PSD into message packets that are communicated to the remote computer system.

The Office Action does not cite DiGiorgio or Elgamal for disclosing features (1) and (2), above. Instead, the Office Action proposes that Graham discloses this subject matter.

More specifically, the Office Action proposes that Graham discloses a system in which a smartcard and server communicate through a host terminal by passing network packets between the smartcard and server that contain APDUs (see Office Action page 3, lines 16-18). Based on this proposed finding of fact and the fact that Graham's network only exists between the server and the host terminal, the Office Action draws the inference that Graham's host terminal: (a) dis-encapsulates APDUs from network packets received from the server and communicates the APDUs to the smartcard and (b) encapsulates APDUs received from the smartcard within network packets to be communicated to the server (see page 3, line 19, through page 4, line 1).

However, Graham does not disclose the proposed finding of fact upon which the Office Action draws its inference. More specifically, Graham does not disclose communicating network packets containing APDUs. Instead, the portion of Graham's disclosure cited by the Office Action in support of the proposed finding states that a server 1310 has a hardware security module (HSM) 1312 that communicates instructions and code 1314 over a network 1320 to a smartcard 212' via a host terminal (see Graham col. 22, lines 54-56 and 63-67). The application code 1314 may be written in JAVA, assembly language, Visual Basic, or C programming language (see col. 23, lines 15-20).

Nowhere does Graham imply or expressly disclose that: (i) information to be communicated from the server to the smartcard exists in the form of a packetized APDU when received by the host terminal or (ii) information to be communicated from the smartcard to the server exists in the form of a packetized APDU when transmitted by the host terminal to the server. Applicants respectfully submit that the Office Action relies entirely on the hindsight afforded by Applicants' specification to find a teaching to modify the prior art to achieve the claimed subject matter.

And although the Office Action proposes that modifying DiGiorgio's system in light of Graham's teachings would provide multi-application secure token devices that are customizable for unique variations of applications after the issuance of the token (see Office Action page 4, lines 1-6), such a modified system is achievable without regard to whether: (i) information to be communicated from a server to a token exists in the form of a packetized APDU when received by a host terminal or (ii) information to be communicated from the token to the server exists in the form of a packetized APDU when transmitted by the host terminal to the server.

Simply stated, information transmitted over a network between a host terminal and a server need not exist in the form of a network packetized APDU for the information to be understood by the receiving device. And none of DiGiorgio, Graham, and Elgamal expressly disclose or suggest a reason for achieving the claimed subject matter of: (1) separating encapsulated APDUs from message packets that are received over a network from a remote computer system and communicating the separated APDUs to a PSD, and (2) encapsulating APDUs received from the PSD into message packets that are communicated over the network to the remote computer system.

Accordingly, Applicants submit that DiGiorgio, Graham and Elgamal, considered individually or in combination, do not render obvious the subject matter defined by claim 1. Independent claims 20, 29, and 42 similarly recite the above-mentioned subject matter distinguishing apparatus claim 1 from the applied references, but with respect to methods.

Therefore, the obviousness rejections applied to claims 18 and 40 are obviated and allowance of claims 1, 20, 29, and 42 and all claims dependent therefrom, is warranted.

To promote a better understanding of the patentable distinctions of the Applicants' claimed subject matter over the applied references, the Applicants provide the following additional remarks.

Although DiGiorgio discloses, in Fig. 1, a secure token device 10 and a client computer system 14 that communicate APDUs to one another (see DiGiorgio col. 9, lines 1-4) and a remote server 16 and secure token device 10 that communicate via a client computer 14 (see abstract lines 1-5), nowhere does DiGiorgio disclose that remote server 16 and secure token device 10 communicate APDUs between one another via client computer 14. The Office Action cites DiGiorgio's column 2, lines 16-23, column 10, lines 24-35, and Figure 8B in relation to the claimed subject matter.

DiGiorgio discloses in column 2, lines 16-23, that a user enters a PIN that is compared to a stored PIN in a secure token device and, if a match occurs, the user is granted access to a local computer system 14, as specified in column 10, lines 1-11. All such functions are carried out locally between computer system 14 and a secure token device 10. There is no involvement of an ISP or a remote server 16.

DiGiorgio's figure 8B illustrates a response APDU that is described in column 9, lines 35-43, and concerns only communications between the secure token device and local computer system 14 using an Opencard API stored on local computer system 14 and a Javacard API stored in the secure token device (see DiGiorgio col. 7, line 19, through col., line 43).

In fact, DiGiorgio's disclosure in column 7, line 19, through column 9, line 43, makes it clear that communication using APDUs (whether command or response APDUs) takes place only between the secure token device and local computer system 14 (see DiGiorgio col. 8, lines 16-19). Local computer system 14 and the secure token device operate according to a master-slave model and "the secure token device 10 always waits for a command APDU from the computer system by way of the reader 12" (see col. 9, lines 6-10). Communication using APDUs does not occur between the ISP/remote server 16 and local computer system 14.

In fact, DiGiorgio discloses that remote server 16, controlled by the ISP, provides access to the Internet and is linked to computer system 14 via a communication link 16 (see col. 5, lines 50-57). A web browser 72 is provided in a primary storage 68 at local computer system 14 to access the Internet and processes HTML documents (see col. 7, lines 44-50). This would imply that communication occurs using a protocol such as Hyper Text Transfer Protocol, for example.

Consequently, communication between secure token device 10 and ISP/remote server 16 occurs in at least two separate steps: (1) ISP/remote server 16 communicates with local client computer system 14 via a communication link 15; and (2) local client computer system 14 performs data translation and communicates with secure token device 10 using the Opencard standard, as stated at column 5, lines 26-37, and further explained below with respect to column 10, lines 24-53.

DiGiorgio discloses in column 10, lines 24-53, obtaining user access to services provided by an internet service provider (ISP) by double clicking an icon, associated with the ISP, on the client which initiates a two-way challenge response, where access is provided to the ISP services following a positive outcome of the two-way challenge response. Neither this column nor any other column of DiGiorgio discloses communicating APDUs from a server/remote computer and over a network to a client. In DiGiorgio, APDUs are solely communicated between security token device 10 and the local client/computer system.

In column 10, lines 24-45, DiGiorgio discloses that a user accesses services of the ISP by double clicking an icon of the computer system. A two-way challenge response authentication is then initiated where the ISP issues a challenge to the secure token device. The secure token device responds and, if the response is proper, the user is authenticated and the secure token device issues a challenge to the ISP. However, with respect to communications between the secure token device and the ISP related to the challenge response authentication, the only detail specified is that "The ISP applet 44 contains the appropriate intelligence for responding to such a challenge. The challenge may be issued by one of the applications 78 stored in the primary storage 68 of the computer system." Consequently, it can only be concluded from what is disclosed at column 5, lines 33-37, and column 7, line 19, through column 9, line 43, that the Opencard API 76 in association with another Java applet (see col. 7, lines 50-56) contained in local computer system 14 interacts with ISP applet 44 in the secure token device and passes APDU commands to ISP applet 44 and the ISP applet 44 replies by passing APDUs or APDU responses to the Java applet and the Opencard API 76, as is normal in the Opencard standard, in order to carry out the challenge response authentication.

Thus, it is a Java applet and an API running on local computer system 14 that carries out the challenge function, to generate and send APDUs to secure token device 10 and to receive APDUs from secure token device 10. The ISP does not generate APDUs, or send APDUs, or send APDUs in an encapsulated message to local computer system 14. Such a capability is only possible at local computer system 14, as disclosed at column 7, line 19, through column 9, line 43. Such a capability using the Opencard standard and Javacard API is not described with relation to the ISP or remote sever 16. Consequently, in the absence of such capability being located at the ISP or remote sever 16, the generation of APDUs, or the sending of APDUs or the sending of APDUs in an encapsulated message to local computer system 14 from the ISP or remote server 16 are all impossible. These capabilities and operations are disclosed nowhere in DiGiorgio with respect to the ISP or remote sever 16.

Moreover, the ISP or remote server 16 are not sent response APDUs from local computer system 14 (such as that illustrated in Figure 8B, for example), as local computer system 14 does not have any technical capability to send a response APDU to the ISP or remote server 16 and additionally because the ISP or remote server 16 disclosed in DiGiorgio does not have any technical capability to handle or process such a response APDU if it were to receive a response APDU or encapsulated response. Additionally, it is simply not disclosed in DiGiorgio that response APDUs are communicated from local computer system 14 to remote server 16/ISP. DiGiorgio solely discloses that response APDUs are communicated to the local computer system from the secure token device (see DiGiorgio col. 7, line 19, through col. 9, line 43).

In fact, DiGiorgio is completely silent as to precisely how the challenge response authentication (as disclosed in column 10) is carried out between the ISP and the secure token device and as to how any communications between the ISP and the secure token device is carried out.

Consequently, it can only be concluded from what is actually disclosed in DiGiorgio that the challenge response authentication is carried out first of all via communication from the ISP to local computer system 14 using, for example, a Hyper Text Transfer Protocol (see col. 7, 44-49) via a communications link 16, and then computer system 14 communicates with secure token device 10 using the Opencard standard and a Java applet/API to communicate with ISP applet 44 in secure token device 10, as clearly disclosed at column 5, lines 26-37, and column 7, line 19, through column 9, line 43.

With respect to independent claims 1 and 42, Applicants submit the Office Action's assertion, in relation to DiGiorgio, that "when a user attempts to access ISP services from the token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2 lines 16-23 & Col. 10 lines 24-33)" and "once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10 lines 33-35)" is incorrect in view of the above comments (see Office Action page 3, lines 7-10 and 12-13). And DiGiorgio does not disclose the claimed subject matter of:

"a first client data processing section receiving incoming message packets from said remote computer system using said client communications section, separating encapsulated APDUs from said incoming message packets thus generating desencapsulated APDUs and routing said desencapsulated APDUs to said PSD through said PSD Interface independently of the origin and integrity of said incoming message; and

a second client data processing section receiving incoming APDUs from said PSD interface, encapsulating said incoming APDUs into outgoing message packets and routing said outgoing message packets to said remote computer system through said client communications section."

Furthermore, DiGiorgio's disclosed user does not attempt to access services of the ISP from the token device; this is done by double clicking an icon on local computer system 14 (see DiGiorgio col. 10, lines 24-28).

With respect to independent method claims 20 and 29, Applicants submit that the Office Action's assertion that "when a user attempts to access ISP services from this token device, the ISP issues a challenge to the token device to ensure that the user should be granted access to the ISP services (Col. 2 lines 16-23 & Col. 10 lines 24-33)" and "once the challenge is received at the token device, the token device issues a response to the ISP challenge in the form shown in Figure 8B (Col. 10 lines 33-35)" is incorrect in view of the above remarks (see Office Action, paragraph bridging pages 10 and 11). And DiGiorgio does not disclose the claimed subject matter of:

"converting on said remote computer system said request from said non-native protocol into an APDU format request message using a first server data processing section,

encapsulating on said remote computer system said APDU format request message into said packet based communications protocol producing an encapsulated request message, using a second server data processing section, ...

receiving by said client said encapsulated request message sent over said network, processing said encapsulated request message using a first data processing section to separate said APDU format request message from said encapsulated request message, ...

receiving by said client said APDU format response message through said PSD Interface and encapsulating said APDU format response message into said packet based communications protocol producing an encapsulated response message, using a second data processing section transmitting said encapsulated response message over said network using said packet based communications protocol,

receiving said encapsulated response message sent over said network by said remote computer system, processing said encapsulated response message using a third server data processing section to separate said APDU response message from said encapsulated response message thus generating a desencapsulated APDU response message, and

converting by said remote computer system said desencapsulated APDU response message into a response in a non-native protocol using a fourth server data processing section and forwarding said response to at least one API Level Program."

Moreover, the claimed step of "generating a request to access said PSD on said remote computer system, wherein said request is in a non-native protocol for communicating with said PSD and said request is generated by an API Level Program" is not disclosed by DiGiorgio's "secure token device access system wherein a secure token device and a local computer system communicate via a token reader, and by passing data packages known as application protocol data units (APDUs) using the reader (Col. 1, line 63 - col. 2 line 13 & Col. 9 lines 1 - 6)" (See Office Action page 10) as in the claimed invention the above request is generated at a remote computer system and in DiGiorgio it can only happen at the local computer system locally connected to the reader, as pointed out in the Office Action. The same arguments equally apply to the subject matter of independent claim 29 as it contains similar subject matter to that of claim 20 with the additional features that the APDU format message is encrypted using a cryptography data processing section.

While acknowledging that DiGiorgio does not expressly disclose encapsulating APDUs for communication between client computer 14 and remote server 16 (see Office Action page 4, first paragraph, and page 12), the Office Action considers that it would have been obvious to one of ordinary skill in the art at the time the invention was made to encapsulate the packets transmitted from the local computer to the remote computer in DiGiorgio using SSL in order to provide security in communications over networks that is platform independent, that can work with many different types of applications that request a wide variety of different types of server applications, and which can be performed with minimal time and effort as taught by Elgamal (see Elgamal col. 1, lines 11-19, 36-66).

Elgamal discloses a secure socket application program interface layered between an application layer and a transport layer for encrypting and decrypting information transferred over a network between a client application program running on a client computer and a server application program running on a server computer (see Elgamal col. 1, lines 58-67, col. 2, lines 1-19, col. 13, line 60, through col. 16, line 49).

As such, an SSL data transfer between a client and a remote server includes encapsulation of the data, the Office Action states that a skilled person would have combined the teachings of DiGiorgio and Elgamal "to provide a security in communications over networks that is platform independent, that can work with many different types of applications, that request a wide variety of different types of server applications, and which can be performed with minimal time and effort" and a skilled person would thus have arrived at the subject matter of the claimed invention.

However, as argued in response to the last Office Action, neither DiGiorgio nor Elgamal discloses communicating APDUs between a PSD and a remote computer via a local computer hosting the PSD and a network interfacing the local computer and the remote computer. As a result, it necessarily follows that DiGiorgio and Elgamal cannot disclose encapsulating the APDUs for communication between the local computer and the remote computer.

Moreover, based on the Office Action's assertion that "DiGiorgio does not disclose that the packets transmitted between the local computer and remote computer are encapsulated" (see Office Action page 4), it seems that the Office misunderstands the encapsulation done in the claimed invention.

With the claimed subject matter, the APDU format request messages are encapsulated on the remote computer system producing encapsulated messages which are themselves incorporated into outgoing message packets transmitted over the network using the packet based communications protocol. The message packets are then received by the client and processed to extract the encapsulated message APDUs which are then decapsulated into APDUs which are then routed to the PSD through the PSD interface.

In other words, the APDUs are not directly transported with a network transport protocol like SSL. There is an intermediate level of APDU encapsulation that is never described in the cited documents taken apart or combined.

Therefore, it is submitted that the subject-matter of claim 1 is not obvious over the cited documents considered individually or in combination. Independent claims 20, 29 and 42 similarly recite the above-described features distinguishing apparatus claim 1 from the cited documents, but with respect to methods. Therefore, the subject-matter of these claims is not obvious over the cited documents.

In view of the above, it is submitted that this application is in condition for allowance, and a notice to that effect is respectfully solicited.

If any issues remain which may best be resolved through a telephone communication, the Examiner is requested to telephone the undersigned at the local Washington, D.C. telephone number listed below.

Respectfully submitted,

/James Edward Ledbetter/

James E. Ledbetter
Registration No. 28,732

Date: February 23, 2009
JEL/DWW/att

Attorney Docket No. L741.01101
Dickinson Wright PLLC
1875 Eye Street, NW, Suite 1200
Washington, DC 20006
Telephone: (202) 659-6966
Facsimile: (202) 659-1559